

Amendments to the drawings,

There are no amendments to the Drawings.

Remarks

Status of application

Claims 1-64 are pending in the application. Claims 1-64 stand rejected on the basis of prior art. In view of the remarks made below, re-examination and reconsideration of the claims are respectfully requested.

The invention

Applicant's invention comprises a system providing for a security component on client premises equipment (e.g., a router) to check compliance of a client computer with an access policy before permitting the computer to access the Internet (e.g., Applicant's specification, page 19, lines 22-27). Applicant's system delegates a portion of the overall operation of a security solution to a local piece of client premises equipment which enforces compliance by client computers with an access policy governing Internet access (e.g., Applicant's specification, page 19, lines 19-27). Every few seconds a security component of the present invention on client premises equipment (e.g., Fig. 3 at 310, 311) sends a communication referred to as a "router challenge" to computers on the local network (e.g., Applicant's specification, page 20, lines 23-24; Fig. 3 at 320, 330, 340). The router challenge requests a response from the local computers (Applicant's specification, page 20, lines 24-25). At the local computers, a client-side security component of the present invention prepares and returns a response to the router challenge (e.g., Applicant's specification, page 25, lines 19-22; Fig. 3 at 321, 341). The responses to the router challenge that are received (if any) are stored in the router compliance table (e.g., Applicant's specification, page 21, lines 10-12; Fig. 3 at 312).

Each time the client premises equipment receives a request to connect to the Internet from a particular computer, its security component determines evaluates the responses in the router compliance table to determine whether or not the particular computer properly responded to the most recent router challenge (e.g., Applicant's specification, page 21, lines 12-15; Fig. 3 at 311, 312). If the computer properly responded to the challenge and was determined to be in compliance with the access policy, then the security component on the client premises equipment permits the

computer to access the Internet (e.g., Applicant's specification, page 21, lines 15-18). However, if the computer did not answer the router challenge or responded with information indicating that it was not in compliance with the access policy, then it is not allowed to connect to the Internet (e.g., Applicant's specification, page 21, lines 19-26). Instead, the non-compliant computer is redirected to a "sandbox" server to address the non-compliance (e.g., Applicant's specification, page 21, lines 26-30; Fig. 3 at 313, 330, 360). The non-compliant computer is only permitted to connect to the sandbox server for performing a defined set of tasks and all other Internet access by the non-compliant computer is disabled (e.g., Applicant's specification, page 21, lines 28-30).

Prior Art Rejections

A. General

The Examiner has issued a final rejection of Applicant's claims relying primarily on U.S. Patent No. 6,463,474 B1 issued to Fuh et al (hereinafter "Fuh"). Applicant acknowledges that as Examiner has issued a final action, the Examiner is not required to consider this Response After Final. However, Applicant is submitting this Response After Final in order to clarify Applicant's arguments as Applicant believes that the Examiner overlooked several important distinctions between claim limitations of Applicant's claims and the teachings of Fuh and the other prior art references. As will be shown below, Applicant's invention as defined in Applicant's independent claims 1 and 45 (as well as other claims) contain elements which are not found in the prior art references cited by the Examiner. The deficiencies of these prior art references with respect to the specific limitations of Applicant's claims are described in detail below.

B. Claim Rejections under 35 USC Section 102

Claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,463,474 B1 issued to Fuh et al (hereinafter "Fuh"). Initially, it should be noted that the Examiner has not included claims 9 and 22 in the list of claims rejected as anticipated by Fuh at paragraph 2 at page 2 of the Office Action mailed April 7, 2005 (hereinafter "Second Office Action"). However, it will be assumed that the Examiner meant to include claims 9 and 22 in this

list of claims rejected as anticipated by Fuh as the Examiner has so indicated at paragraph 6 at page 6 and at paragraph 2 at page 4 of the Second Office Action, respectively. If the foregoing assumption is incorrect, further clarification as to the basis for rejection of claims 9 and 22 is requested.

The following rejection of Applicant's claim 1 by the Examiner is representative of the Examiner's rejection of the Applicant's claims of this group as being anticipated by Fuh:

With respect to claim 1, Fuh et al discloses: In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #2 10, item #216), a method for managing Internet access based on a specified access policy (see abstract), the method comprising: transmitting a challenge from said client premises equipment to each client computer (figure 4 item #403), for determining whether a given client computer is in compliance with said specified access policy; transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued (figure 4 item #404); and blocking Internet access for any client computer that does not respond appropriately to said challenge (figure 7A block #707).

(Second Office Action, paragraph 2, page 2)

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, Fuh fails to teach each and every element set forth in claims 1 and 45 (as well as other claims) and therefore fails to establish anticipation of the claimed invention under Section 102.

The Examiner equates Fuh's firewall router which authenticates users with Applicant's security system which provides for client premises equipment (e.g., a router) to regulate access to the Internet by client computers based on an access policy. At the outset, Applicant does not claim to have invented the notion of authenticating a user at a router. To be sure, at a high level both Fuh's system and Applicant's invention involve routers (or other similar client premises equipment). However, Applicant's claimed invention includes specific elements that distinguish it from Fuh's system. As described below, Fuh's system decides whether to authenticate a user for access to particular

resources (e.g., an intranet) based on user login information, while Applicant's security system serves a different purpose in enforcing compliance by client computers with an access policy governing Internet access by the client computers. The differences between Applicant's invention and Fuh's system become apparent when the elements of Applicant's claims are compared to the specific teachings of Fuh cited by the Examiner. As a first example, the Examiner references Fuh's abstract for the teaching of "a method for managing Internet access based on a specified access policy" as stated in Applicant's claim 1. However, Fuh's abstract describes a router that intercepts traffic from a client directed towards a network resource for purposes of authenticating the client (i.e., user) at the router. It does not describe an access policy for managing Internet access by client computers. The Examiner also references Fuh at col 6, lines 1-5 for the teaching of the comparable element of Applicant's claim 45 of "an access policy governing Internet access by client computers". However, this portion of Fuh reads as follows:

...the invention encompasses a computer system for controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource, comprising ... creating and storing client authorization information at the network device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and what access privileges the client is authorized to have with the network resource.

(Fuh, col 5, line 58 - col. 6, line 5, emphasis added)

Fuh's authentication proxy is implemented at a firewall router which protects a particular network resource from access by external user(s). Fuh's system is focused on protecting this particular resource (e.g., server on an intranet serving a given organization). If an external user seeking to access the particular network resource is authenticated by Fuh's system, then the system also indicates what access privileges the user is authorized to have with the particular network resource. The "access privileges" that are given to users by Fuh's system relate to the particular network resource. Applicant's access policy, in contrast, relates to Internet access by client computers and not to a particular network resource. Another significant difference is that Fuh's "access

privileges" (or "user profile") are applied to a particular user after the decision about whether or not to authenticate the particular user for access to the network resource is made (Fuh, col. 7, lines 56-58). This is not Applicant's approach. Applicant's access policy is not applied after the decision to permit access is made. Instead, Applicant's system examines compliance with the access policy in making the decision about whether to permit access. For these reasons, Fuh's access privileges are not comparable to Applicant's claim element of "managing Internet access based on a specified access policy" which governs Internet access by client computers.

Another major difference between the system of Fuh and that of Applicant is that the "challenge" issued by Fuh's system requests login information for authentication of a user. Applicant's invention, in contrast, issues a challenge to a client computer for determining whether the client computer is in compliance with the above-described access policy governing Internet access by client computers. The Examiner references the arrow 403 at Fig. 4 of Fuh for the teaching of determining whether a client computer is in compliance with an access policy. However, the following description of this arrow 403 in the Fuh reference clearly indicates that the purpose of this "challenge" is to obtain user login information:

Referring again to FIG. 7B, after the new authentication cache is created, login information is requested from the client, as shown in block 724. For example, Authentication Proxy 400 obtains authentication information from User 302 by sending a login form to client 306. The login form is an electronic document that requests User 302 to enter username and password information, as shown by path 403.

(Fuh, col. 11, lines 49-55)

As illustrated above, Fuh's system is focused on authenticating a user based on login information (e.g., username and password), rather than based on compliance of the client computer with an access policy governing Internet access. The "challenge" issued by Fuh's authentication proxy requests a user to enter a username and password in a login form. Fuh's system determines whether or not to permit remote access to particular resources (e.g., intranet) based on this user login information. If the login information

supplied by the user is correct and the authentication process is successful, access is permitted and the authentication cache is updated so that subsequent requests can authenticate at the firewall router without consulting a separate authentication server (Fuh, col. 12, lines 38-47).

Unlike Fuh's system, Applicant's invention does not permit or block requests for access based on user login information. Instead, Applicant's system determines whether a given client computer is in compliance with the specified access policy governing Internet access. If the client computer is not in compliance with the access policy, Applicant's invention blocks access to the Internet. These features are specifically described in Applicant's claims, including, for example, in Applicant's claim 1 which includes the following claim limitations:

1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
transmitting a challenge from said client premises equipment to each client computer for determining whether a given client computer is in compliance with said specified access policy;
transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and
blocking Internet access for any client computer that does not respond appropriately to said challenge.

(Applicant's claim 1, emphasis added)

As shown above, Applicant's invention provides for client premises equipment to regulate access to the Internet by client computers. The decision about whether to allow Internet access by a given computer is based on compliance by the given computer with the above-described access policy. This is different than Fuh's approach which teaches authenticating a user for access based on login information (e.g., user name and password) supplied by the user.

Another difference between Applicant's approach and that of Fuh is that Applicant's system provides for blocking access by the client computer to the Internet, while Fuh's system focuses on blocking external access to particular resources (e.g., an

intranet server). Fuh's system is implemented in a firewall router which provides for examining incoming attempts from external sources to access a particular network resource (e.g., server on intranet). Applicant's invention, in contrast, provides for local client premises equipment to enforce compliance by client computers with the access policy governing Internet access. This is specifically indicated in claim 1 which includes the following claim limitations:

In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

(Applicant's claim 1, emphasis added).

The Examiner references Fig. 3, item 210 and the login arrow 402 shown at Fig. 4 of Fuh for the corresponding teaching of client premises equipment serving a routing function for each client computer to be regulated which issues a challenge to client computers. However, Fuh describes a firewall router which regulates remote access to particular resources (i.e., the intranet 216) as illustrated by the following:

The firewall router 210 is coupled to intranet 216, and an authentication and authorization server 218 ("AAA server"). The firewall router 210 controls remote access to intranet 216.

(Fuh, col. 8, lines 25-28, emphasis added)

As shown at Fig. 2, in Fuh's system the LAN 206 and intranet 216 are located in logically distinct regions (Fuh, Fig. 2). The LAN 206 is located in a first region 202 and the intranet 216 is located in the second region 204, which may be geographically separate (Fuh col. 8, lines 14-19). Applicant's invention, in contrast, provides for the access policy governing Internet access by client computers to be enforced by client premises equipment serving a routing function for the client computers that are being

regulated, such as a router on the local LAN. If a given client computer is not in compliance with the access policy, access to the Internet by the client computer is regulated (i.e., selectively blocked). These limitations of client premises equipment regulating Internet access by a client computer based on whether the client computer is in compliance with an access policy are also recited in Applicant's claim 45, as follows:

A system for regulating Internet access by client computers comprising:
an access policy governing Internet access by said client computers;
client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a challenge to each client computer, for determining whether a given client computer is in compliance with said access policy;
an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.

(Applicant's claim 45, emphasis added)

Additional distinctions between Applicant's invention and that of Fuh are illustrated in Applicant's dependent claims. For example, Applicant's claim 12 includes the following claim limitations:

The method of claim 1, wherein said access policy specifies applications that are allowed Internet access.

(Applicant's claim 12)

As shown above, Applicant's claimed approach involves an access policy which specifies particular applications which are allowed Internet access. Applicant's claims 11 and 55 also include similar claim limitations. The Examiner references Fuh at column 7, lines 56-58 for the teaching of an access policy specifying applications that are allowed Internet access. However, the referenced portion of Fuh reads as follows:

If the username is successfully authenticated, then the firewall is dynamically configured to open a passageway for the HTTP packets as well as other types of network traffic initiated from the user on the client. The other types of network traffic that are permitted through the passageway are specified in a user profile for that particular user.

(Fuh, col. 7, lines 56-58, emphasis added)

As described above, Fuh's system receives identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Fuh's system permits particular types of network traffic initiated by that particular user which are specified in the user's profile. The Examiner states that Fuh's "user profile" for a "particular user" is equivalent to Applicant's claim limitations of an access policy regulating access to the Internet by client computers which specifies applications allowed to access the Internet. However, the teachings of Fuh referenced by the Examiner indicate that Fuh's system decides whether or not to authenticate a user based on user login information and without examination of applications on the client computer. As previously described, the user profile (or access privileges) are applied by Fuh's system only after the decision about whether to permit access is made (i.e., after the user is authenticated). This is not Applicant's claimed approach. Applicant's approach provides for determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access. Applicant's approach provides for making the decision about whether or not to permit access based on the access policy. This is not the same as applying a profile or set of privileges to a user after the decision to permit access to the user has been made.

All told, Fuh's system is distinguishable from that of Applicant on several grounds which are specifically included as claim limitations of Applicant's claims 1 and 45 and other dependent claims thereof. As described above, Fuh provides no teaching comparable to Applicant's claim limitations of an access policy governing Internet access by client computers. Significantly, Fuh's firewall router provides for determining whether or not to authenticate a user for access to particular network resources based on user login information. In contrast, Applicant's invention regulates Internet access based on whether or not a client computer attempting Internet access is in compliance with the specified access policy. Applicant's access policy may also include specific applications which are approved for Internet access. Therefore, as Fuh does not teach or suggest all of the claim limitations of Applicant's independent claims 1 and 45 (and other dependent claims

thereof) it is respectfully submitted that the claims distinguish over this reference and overcome any rejection under Section 102.

C. First Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 under 35 U.S.C. 103(a) as being obvious over Fuh. It should be noted that the Examiner has previously rejected claims 47 and 55 as being anticipated by Fuh under Section 102 (Second Office Action, paragraph 2 at page 5 and paragraph 4 at page 5), and has also mentioned rejecting these claims as being obvious over Fuh under Section 103(a) (Second Office Action, paragraph 8 at page 6 and paragraph 12 at page 9). It will be assumed that the Examiner meant to reject claims 47 and 55 as anticipated by Fuh under Section 102. However, if this assumption is incorrect, further clarification of the basis for rejection these claims is requested.

Under Section 103(a), a patent may not be obtained if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. To establish a prima facie case of obviousness under this section, the Examiner must establish: (1) that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, (2) that there is a reasonable expectation of success, and (3) that the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See e.g., MPEP 2142). As will be shown below, the references cited by the Examiner fail to meet the requisite condition of teaching or suggesting all of Applicant's claim limitations.

As to the claims of this group rejected as obvious over Fuh, the Examiner acknowledges that Fuh does not explicitly disclose elements of these claims, but states that the elements not explicitly disclosed in Fuh would have been obvious to one ordinarily skilled in the art. The Examiner's rejection of Applicant's claims 13-16 as follows is representative of the Examiner's rejection of Applicant's claims as obvious over Fuh:

As per claims 13-16, Fuh et al does not explicitly disclose: application are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MDS cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination.

(Second Office Action, paragraph 14)

Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 are dependent upon Applicant's independent claims 1 and 45 and therefore are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. As described above, Fuh does not teach client premises equipment issuing challenges to client computers for determining compliance of such client computers with an access policy governing Internet access. Additional differences between Applicant's invention and that of Fuh are illustrated in Applicant's dependent claims. For example, Applicant's claim 13 includes as claim limitations that applications approved for Internet access in the access policy are "specified by executable name and version number that are acceptable" (Applicant's claim 13). Applicant's claim 13 also references Applicant's claim 12, which provides that Applicant's access policy governing Internet access specifies applications that are allowed Internet access.

The Examiner acknowledges that Fuh does not provide the specific teaching of an access policy in which applications approved for Internet access are "specified by executable name and version number that are acceptable" as provided in Applicant's claim 13, but states that "it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination" (Second Office Action, paragraph 8, page 8). However, as described above, Fuh teaches that the decision about whether or not to permit access is based on user login information (e.g., user name and password). Thus, examining the

executable name and version number of an application is inconsistent with Fuh's approach as Fuh's system decides whether to authenticate a user and permit access on the basis of user login information. Applicant's system, in contrast, makes the decision about whether or not to permit access based on compliance with the access policy. The access policy, in turn, may specify executable names and version numbers of applications which are allowed Internet access.

Applicant's claim 12 includes limitations providing that an access policy governing Internet access by client computers specifies particular applications which are approved for Internet access. The limitations of claim 13 further provide that that access policy specifies not only those applications approved for Internet access, but also specifies particular executable names and version numbers of the applications approved for Internet access. Fuh's system, in contrast, makes the decision about whether to permit access to a particular user based on user login information. Examining executable names and version numbers of applications is inconsistent with these teachings of Fuh. Thus, it is respectfully submitted that Applicant's claims distinguish over these references and overcome any rejection under Section 103.

D. Second Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 22-25, 27-37, 39, 40, and 42-44 under 35 U.S.C. 103(a) as being obvious over Fuh in view of U.S. Patent No. 5,761,683 to Logan et al. (hereinafter "Logan"). In addition, the Examiner has rejected claim 38 in paragraph 31 at page 12 of the Second Office Action; however, the Examiner has not specifically included claim 38 in the list of claims rejected as obvious based on Fuh in view of Logan. It will be assumed that claim 38 is rejected as being obvious over Fuh in view of Logan. If this assumption is incorrect, further clarification is requested.

As to the claims of this group, the Examiner acknowledges that Fuh does not explicitly disclose the elements of redirecting a client computer that is not in compliance with the access policy to a sandbox server and adds Logan for the teachings of redirecting a client computer not in compliance with an access policy to a particular sandbox server and displaying particular error message pages on the sandbox server in response to communications on particular ports (Second Office Action, paragraph 17, pages 9-10).

Claims 22-25, 27-37, 38, 39, 40, and 42-44 are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. As described above, Fuh teaches authenticating a user based on user login information and not examining compliance by a client computer with an access policy. Logan does not cure the above-described deficiencies of Fuh as it provides no teaching of client premises equipment which monitors and enforces compliance by client computers an access policy governing Internet access. Furthermore, Applicant's review of Logan finds that it does not include the specific limitations set forth in Applicant's claims of redirecting a client determined not to be in compliance with the access policy to a "sandbox" server. These limitations are, for example, provided in Applicant's claim 24 as follows:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;
transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and
redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.

(Applicant's claim 24, emphasis added)

The Examiner references Logan at column 19, lines 63-67 for the teaching of redirecting a URL request to a remote server and Logan at column 7, lines 41-48 for display of an error message to indicate to a user that a request did not succeed. The referenced portions of Logan cited by the Examiner simply discuss conventional steps of handling requests for remotely stored documents by redirecting certain requests to retrieve locally stored copies and sending other requests to a remote web server(s). Logan's system provides for returning either the information (e.g., HTML document, graphical image, FTP file, or other displayable data) or an error message if the attempt to obtain the information does not succeed (Logan, column 7, lines 41-48). This does not teach anything analogous to Applicant's claimed approach of redirecting a client computer determined not to be in compliance with the access policy to a particular

"sandbox server" as provided in Applicant's claims. As the combined references do not teach or suggest all of the claim limitations of Applicant's claims, it is respectfully submitted that the claims distinguish over these references and overcome any rejection under Section 103.

E. Third Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 26 and 41 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Logan, further in view of U.S. Patent No. 6,026,440 to Shrader et al (hereinafter "Shrader"). The Examiner acknowledges that Fuh and Logan do not explicitly disclose the element of permitting a client computer to elect to access the Internet after displaying error messages, but adds Shrader (col. 4, lines 56-57) for the teaching of "returning an error message (e.g., Unauthorized) to the browser and prompting the user for id and password" (Second Office Action, paragraph 18, page 11).

Claims 26 and 41, which incorporate the limitations of Applicant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh and Logan in respect to Applicant's invention. Shrader does not cure the above-described deficiencies of Fuh and Logan. The referenced portion of Shrader simply provides that a check is made for credentials of a user and, if the user does not have appropriate credentials, Shrader's system returns an error message and requests username and password from the user. In other words, Shrader's system requires the user to resubmit the credentials and denies access until the proper credentials are received. This does not teach Applicant's claim limitations of client premises equipment which evaluates and enforces compliance by client computers with an access policy, nor does it provide the specific teaching of Applicant's claims 26 and 41 of permitting a client computer not in compliance with the access policy to elect to proceed with Internet access notwithstanding the failure to comply with the access policy. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

F. Fourth Rejection under 35 USC Section 103(a)

The Examiner has rejected claim 61 under 35 U.S.C. 103(a) as being obvious over

Fuh in view of US Patent No. 6,542,933 to Durst, Jr. et al (hereinafter "Durst"). Claim 61, is believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. Durst does not cure these deficiencies. The referenced portions of Durst simply discuss receiving a URL request at an information server and redirecting the request to a content server to receive a content file. Durst provides no teaching of issuing challenges for evaluating compliance of a client computer with an access policy or for redirecting client computers determined not to be in compliance with the access policy to a sandbox server as provided in Applicant's claims. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

G. Fifth Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 62-64 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Durst, further in view of Shrader. These claims, which incorporate the limitations of Applicant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh, Durst and Shrader in respect to Applicant's invention. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

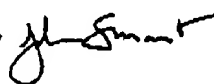
Conclusion

In view of the foregoing remarks, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: June 8, 2005

✓  Digitally signed by John A. Smart
Signature Valid Date: 2006.06.08 12:01:34 -0700

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX